ACLU
AMERICAN CIVIL LIBERTIES UNION of MONTANA

American Civil Liberties Union
of Montana
Power Block, Level 3
PO Box 1317
Helena, Montana 59624
406-443-8590
www.aclumontana.org

January 20, 2009

SB 154

For the record, my name is Scott Crichton. I have been privileged to serve as Executive Director of the American Civil Liberties Union of Montana since 1988. The ACLU is a non-partisan membership based organization with some 2,000 households as members in Montana. We are an affiliate of the national ACLU which has some 550,000 members.

Simply put, ACLU's mission is to defend the Constitution and the Bill of Rights.

The ACLU of Montana is urging Montana's Department of Justice to better protect the privacy of drivers who apply for a new border-crossing license. We urge you to consider a set of recommendations, whether in statute or administrative rules, drafting procedures for implementing the state's new Enhanced Driver's License. Montanans should not have to trade their privacy or the safety of their personal information to make it easier to travel abroad.

Should you pass SB 154, Montana will become one of a few states to offer an Enhanced Driver's License as an alternative to getting a passport. Applicants must provide documentation of citizenship which will be copied and kept on file at the DOL. The enhanced license will display citizenship status and will enable the holder to cross into and return from Canada. The program is voluntary. Traditional "non-enhanced" driver's licenses will remain available.

However, the enhanced licenses use RFID, a technology that could expose users to tracking or monitoring. The RFID in the enhanced licenses will broadcast an individually unique number over a radio frequency to allow Customs and Border Protection to identify approaching drivers.

The ACLU is concerned that without technological safeguards, anyone, at any place, could read the personal identification number being broadcast, without the cardholder ever knowing or consenting. If the personal identification number becomes connected with the cardholder's name, the risk for tracking or monitoring away from the border by the government or anyone else increases.

RFID safeguards such as encryption (to encode the data) or shielding (to keep the number from being broadcast) would help. However, without such protections, cardholders could be tracked by number when not at the border. The ACLU is opposed to the use of RFID in identity documents, but is not challenging this program primarily because of its voluntary nature.

We would like the Department of Licensing to fully inform enhanced license applicants about the privacy risks raised by using RFID. In addition, the state should inform users about the consequences of disabling the RFID in the licenses. And the ACLU is urging that the Department fully describe the safeguards it is implementing to protect the privacy of users.

January/February 2009

RFID's Security Problem

Are U.S. passport cards and new state driver's licenses with RFID truly secure?

By Erica Naone

Starting this summer, Americans will need passports to travel to Canada, Mexico, Bermuda, and the Caribbean--unless they have passport cards or one of the enhanced driver's licenses that the states of Washington and New York have begun to issue.

Valid only for trips by land and sea, these new forms of identification are a convenient, inexpensive option for people who don't need to travel by plane. U.S. passport cards, which were introduced in July, cost about half as much as a full passport, and the extra cost of getting an enhanced driver's license rather than a regular one is even lower. Enhanced licenses have been available in Washington since January 2008 and in New York since September; other border states, including Michigan, Vermont, and Arizona, intend to offer them as well.

But not everyone is convinced that the new IDs are a good idea. The passport card and the enhanced licenses contain radio frequency identification (RFID) tags, which are microchips fitted with antennas. An RFID reader can radio a query to the tag, causing it to return the data it contains--in this case, an identification number that lets customs agents retrieve information about the cardholder from a government database. The idea is that instant access to biographical data, a photo, and the results of terrorist and criminal background checks will help agents move people through the border efficiently. RFID technology, however, has been raising privacy concerns since it was introduced in product labels in the early 2000s.

Meanwhile, although experts say that some RFID technologies are quite secure, a University of Virginia security researcher's analysis of the NXP Mifare Classic *(see Hack, November/December 2008)*, an RFID chip used in fare cards for the public-transit systems of Boston, London, and other cities, has shown that the security of smart cards can't be taken for granted. "I think we are in the growing-pains phase," says Johns Hopkins University computer science professor Avi Rubin, a security and privacy researcher. "This happens with a lot of technologies when they are first developed."

Borderline Security

The first of the new ID cards to be introduced, the federal passport cards and the Washington driver's licenses use similar technology, which has been reviewed and approved by the U.S. Department of Homeland Security. The cards' RFID devices, called electronic product code (EPC) tags, are much like bar codes. The tags are inexpensive and can, in ideal conditions, be read from about 150 feet away--an unusually long range for RFID, says Ari Juels, director and chief scientist at RSA Laboratories in Bedford, MA, which collaborated with researchers from the University of Washington to evaluate both cards.

Although the cards don't store personal information, the researchers concluded that even storing a unique number raises some privacy concerns. "If you think about the Social Security number, at some point there could have been an argument that it's just a number, not personal information," says Tadayoshi Kohno, an assistant professor of computer science at the University of Washington, who participated in the study. "But numbers evolve over time, and uses evolve over time, and eventually these things can reveal more information than we initially expect." What's more, relatively common RFID readers, such as those used for inventory control, could under some circumstances read the cards' numbers from quite a distance. The researchers felt there was a risk that the cards could be used to track people, the way a few shopping centers in Britain have used signals from cell phones to track customers' shopping habits and monitor how long they stay in stores. Although people carry other cards and devices that could also be used for tracking, the researchers note that the identification cards can be read at longer range than many other RFID tags and that people are likely to carry them at all times, while they might leave, say, their cell phones at home. And regular U.S. passports, which also contain RFID chips, use technology that makes privacy problems less likely. Passports, unlike passport cards, must be read from up close, and they have a security system that requires an official to optically scan characters from the document in order to gain access to the personal data stored in the chip.

Gigi Zenk, a spokesperson for the Washington State Department of Licensing, says that Washington has made it illegal for third parties to use data from RFID tags without the tag owners' consent. She and other officials add that anyone concerned about privacy can use the privacy sleeves provided with the cards, which are designed to block radio signals so that the cards are harder to read surreptitiously. But the Washington study showed that the sleeves didn't always work: they didn't block radio signals when crumpled, for instance. The researchers also argued that most people are unlikely to use the sleeves, anyway. Even some privacy researchers Juels consulted confessed to having lost them, he says.

And privacy isn't the only issue here: the researchers say that unauthorized reading would threaten border security as well. If it's easy to get the identification number out of the cards, then it's relatively easy to counterfeit them, simply by loading a stolen ID number onto a blank, off-the-shelf chip. If each RFID chip also had a unique, hardwired serial number, which had to correspond to the stored ID number, it would be harder to counterfeit. But neither the Washington licenses nor the passport cards have that extra security feature.

The Washington cards are open to one additional type of attack: EPC tags can be disabled when a reader issues a "kill" command. Although each tag is designed to be protected by a PIN that allows only authorized users to issue the command, the state never set the PIN on the cards it distributed, allowing anyone with an RFID reader to set it himself and commence killing cards. If a good number of Washingtonians with enhanced licenses were gathered at a border crossing, someone could cause a disruption by killing large numbers of cards. An attacker could also use this tactic to harass particular individuals, since a killed card is likely to draw suspicion.

Juels is quick to note that the cards won't be the only thing protecting the border. "If border agents do all that they're supposed to do [including, for example, comparing the photographs stored in the database with those printed on the ID], they should be able to detect counterfeits," he says. He adds, however, that it's human nature to become less vigilant when there's technology to lean on.

When I asked the Department of Homeland Security about these concerns, press secretary Laura Keehner responded with a statement that said, in part, "While the risks described in the University of Washington/RSA paper may be technically possible, we believe that many are - improbable, and even if realized, would have little impact other than causing an individual traveler minor inconvenience at the border. ... As we identify additional mitigation strategies, we will continue to strengthen requirements for ... cross-border travel documents in order to both enhance border security and privacy of the document holder."

The New York License, and Beyond

No independent researcher has yet published an evaluation of New York's enhanced driver's license, but the card avoids some of the concerns raised about the federal and Washington cards. The chips in the New York licenses have serial numbers to protect them against counterfeiting, and their memory banks have been locked to protect them against unauthorized use of commands. It's admirable that Homeland Security and the states it's working with are willing to make use of better technologies than they chose at first. But it's not clear whether these efforts will go far enough.

The New York licenses present the same privacy issues that the other cards do, and as Keehner's comments suggest, officials have a tendency to dismiss such concerns--which could very well mean that nothing will be done about them. Yet surely it's possible to protect the privacy of cardholders without requiring them to keep track of privacy sleeves. For example, says Avi Rubin, each card could be fitted with a button that allows the user to control when to send information. Unless the button was pushed in, the ID wouldn't respond to queries. Such cards would cost a bit more, but they could offer more security as well as more privacy.

As long as the remaining problems are ignored, though, it's unlikely that the technology will become good enough to protect international borders without compromising the privacy of thousands or millions of people. Tadayoshi Kohno, for one, says that at this point, he is not convinced that RFID even offers security advantages over the old IDs. Technology used on this scale, and for purposes this important, should be clearly better than what it's replacing: the U.S. experience with electronic voting systems shows what can happen when it's not. If officials continue to advocate band-aids such as privacy sleeves rather than working to address the full extent of critics' concerns, they will ultimately undermine the very technology that they hope to promote. While new ID technology seems likely to stay, it could become a fiasco if officials don't pay attention to the work of hackers and security researchers. These people try to expose weaknesses before they can be exploited maliciously. It's much less painful to swallow the news from them than to wait until a problem becomes embarrassing--or devastating.

Erica Naone is a *Technology Review* assistant editor.